United States District Court

SOUTHERN DISTRICT OF FLORIDA

In the Matter of the Search of
(Name, address or brief description of property or premises to be searched)

Residence located at:
7611 U.S. Highway 27 South
Sebring, Highlands County, FL
(More fully described in Attachment A)

SEARCH WARRANT

CASE NUMBER: 06-13-FJL

TO: Brian P. Ray, Immigration and Customs Enforcement, and any Authorized Officer of the United States, an Affidavit having been made before me by Special Agent Brian P. Ray, who has reason to believe
(Affiant)

that on the _____ person of or ____X____ on the premises known as
(name, description and/or location)

SEE ATTACHMENT A

in the SOUTHERN District of FLORIDA there is now concealed a certain person or property, namely (describe the person or property)

SEE ATTACHMENT B

I am satisfied that the affidavit(s) and any recorded testimony establish probable cause to believe that the person or property so described is now concealed on the person or premises above-described and establish grounds for the issuance of this warrant.

YOU ARE HEREBY COMMANDED to search on or before _____
(not to exceed 10 days) the person or place named above for the person or property specified, serving this warrant and making the search (in the daytime - 6:00 A.M. to 10:00 P.M.)(at any time in the day or night as I find reasonable cause has been established)) and if the person or property be found there to seize same, leaving a copy of this warrant and receipt for the person or property taken, and prepare a written inventory of the person or property seized and promptly return this warrant to Frank J. Lynch, Jr. United States Magistrate Judge as required by law.
U.S. Judge or Magistrate Judge

March _____, 2006
Date and Time Issued

at Fort Pierce, Florida
City and State

FRANK J. LYNCH, JR.
UNITED STATES MAGISTRATE JUDGE
Name and Title of Judicial Officer

_____
Signature of Judicial Officer

AFFIDAVIT
OF
BRIAN P. RAY
SPECIAL AGENT
U.S. IMMIGRATION AND CUSTOMS ENFORCEMENT

I, Brian P. Ray first being duly sworn, does hereby depose and state as follows:

INTRODUCTION AND BACKGROUND

1. I, Brian P. Ray, am a Special Agent employed by U.S. Immigration and Customs Enforcement (ICE). I have been a Federal Agent assigned to the investigations office in Ft. Pierce, Florida since October 2001.

2. I am responsible for enforcing Federal Criminal Statutes relating to Immigration and Customs Enforcement, including the title and section prohibiting the distribution of child pornographic materials, to wit: Title 18, United States Code, Section 2251-57, along with any/all violations under Title 18.

3. This Affidavit is made in support of an application for a search and seizure warrant, to search and seize data and evidence from the residence of Alicia and Paul Peters, 7611 U.S. Highway 27 South, Sebring, Florida.

4. I have received over 700 hours of training in the application of Federal Statutes, including child pornography investigations, Federal Court procedures and the techniques required to insure the admissibility of evidence at trial.

Forensic Analysis of Computers

5. I consulted with SSA David Sheeks, RAC/Ft. Pierce ICE computer forensics agent. SSA Sheeks advised the following; based upon his knowledge, training and experience, and that of the Computer Forensics Unit at the ICE Cyber Crimes Center (IC3), computer files or remnants of such files can be recovered months or even years after they have been accessed by a computer. Electronic files downloaded to a hard drive can be stored for years at little or no cost. Even when such files have been deleted, they can be recovered months or years later using readily available forensics tools. When a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the hard drive (or media) until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space - that is, in space on the hard drive (or media) that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space - for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file. Similarly, files that have been viewed via the Internet are automatically downloaded into a temporary Internet directory or "cache." The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only

overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer habits.

6. SSA Sheeks has advised that based upon his knowledge, training and experience, and that of the Computer Forensics Unit at IC3, searching and seizing information from computers often requires agents to seize most or all electronic storage devices (along with related peripherals) to be searched later by a qualified computer technician in a laboratory or other controlled environment. This is true because of the following;

(a) Volume of evidence: Computer storage devices (like hard disks, diskettes, tapes, and optical disks) can store the equivalent of millions of pages of information. Additionally, a suspect may try to conceal criminal evidence; he or she might store it in random order with deceptive file names. This may require searching authorities to examine all the stored data to determine which particular files are evidence or instrumentalities of crime. This process can take weeks or months, depending on the volume of data stored, and it would be impractical and invasive to attempt this kind of data search on-site.

(b) Technical requirements: Searching computer systems for criminal evidence is a highly technical process requiring a properly controlled environment. The vast array of computer hardware and software available requires that some computer technicians specialize in particular systems and applications, so it is difficult to know

before a search which technician is prepared to analyze the system and its data. In any event, data search protocols are exacting scientific procedures designed to protect the integrity of the evidence and to recover even hidden, erased, compressed, password-protected, or encrypted files. Because computer evidence is vulnerable to inadvertent or intentional modification or destruction (both from external sources and from destructive code imbedded in the system as a "booby trap"), a controlled environment is necessary to complete an accurate analysis. Further, such searches often require the seizure of most or all of a computer system's input/output peripheral devices, related software, documentation, and data security devices (including passwords) so that a qualified computer technician can accurately retrieve the system's data in a laboratory or other controlled environment.

(c) Networked computers: In computers that are networked, data from one computer may be retrievable from other computers on the local network. This may occur as a result of one computer backing up and/or sharing files with other computers on the network. Networked computers may also share printers resulting in data from one computer being retrievable from the other(s).

7. In light of these concerns, I hereby request the Court's permission to seize all computer hardware (and associated peripherals/media/software/documentation) that is capable of containing or being used to access/produce some or all of the evidence described in the warrant, and to conduct an off-site search of the seized items for the evidence described.

8. I am familiar with all the facts and circumstances surrounding this investigation as set forth herein, both from my

own investigative efforts and from information obtained from other law enforcement officers with personal knowledge of the evidence and activities described herein.

APPLICABLE LAW

9. For purposes of reference herein, I am aware that 18 U.S.C. § 2252(a)(2) prohibits knowingly receiving, or distributing, any visual depiction that has been mailed, or has been shipped or transported in interstate or foreign commerce, or which contains materials which have been mailed or so shipped or transported, by any means including by computer, or knowingly reproduces any visual depiction for distribution in interstate or foreign commerce or through the mails, if -

- the producing of such visual depiction involves the use of a minor engaging in sexually explicit conduct; and,
- such visual depiction is of such conduct.

Additionally, 18 U.S.C. § 2252(a)(4)(B) prohibits knowingly possessing one or more books, magazines, periodicals, films, video tapes, or other matter which contain any visual depiction that has been mailed, or has been shipped or transported in interstate or foreign commerce, or which was produced using materials which have been mailed or so shipped or transported, by any means including by computer, if:

- the producing of such visual depiction involves the use of minor engaging in sexually explicit conduct; and,
- such visual depiction is of such conduct,

Title 18, United States Code, Section 2256(1) defines "minor" as "any person under the age of 18 years." Title 18, United States Code, Section 2256(2)(A) defines "sexually explicit conduct" as actual or simulated:

- sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex,
- bestiality,
- masturbation,
- sadistic or masochistic abuse; or,
- lascivious exhibition of the genitals or pubic area of any person.

Title 18, United States Code, Section 2256(5) defines "visual depiction" as including undeveloped film and videotape, and data stored on computer disk or by electronic means which is capable of conversion into a visual image. For purposes of this affidavit, any visual depiction of a minor engaged in sexually explicit conduct as defined in Title 18, United States Code, Section 2256(2), will be referred to as "Child Pornography."

INVESTIGATION

10. On February 2, 2006, SAC/Chicago Senior Special Agent (SS/A) Mary Buduris conducted an Internet investigation utilizing WinMX peer-to-peer software, which is an application that offers a method of direct communication between computers connected via the Internet (also known as "file sharing" programs). Such programs allow for the real-time exchange of computer files (audio, video, images, movies, programs, games, etc) between users. Peer-to-peer programs may typically be downloaded into a person's computer and

then configured by the user to enable the downloading, and/or uploading, of files contained in a user's hard drive. The files to be shared are typically placed into a "shared" folder. WinMX users may choose to make files available online to others, or configure the software so he/she may download files from others, without allowing access to his/her files. If a user's shared folder is made available online, it means the user is offering the files to other persons, worldwide, who are using compatible peer-to-peer software.

11. SS/A Buduris, while acting in an undercover capacity, initiated the WinMX investigation using the persona of "tammiety682". SS/A Buduris entered a WinMX chat room "kiddypics & kiddyvids (adult chat)," and noticed one screen name, "Alex1007" in the same chat room. Screen name "Alex1007" appeared to have a significant amount of files available for download with names indicative of child pornography (See, Attachment C).

12. At approximately 9:03 AM, SS/A Buduris began to download several files from screen name "Alex1007." SS/A Buduris initiated downloads of images and video files titled as follows:

(a) Japanese Lolita child porno(5)11yo primary school girl spreads hairless pussy to how(1)(1)(1)(1)(2).jpg
(b) my daughter alex 13 pussy.jpg,
(c) my daughter alex 13 pussy2.jpg,
(d) young lolita incest porno underage(1)(1) (1).jpg,
(e) pthc the best 9y very slut gets a load of cum in her mouth I love her!!!.jpg,
(f) R@ygold [CHILD]12yo_fuck_she is up.mpg,

(g) pthc 12 - year - 12 yr old handjob and blowjob.mpg.[1]

13. I have reviewed the downloaded files and found that files (a) and (d) appear to be adult pornography. Files (b), (c), (e), and (f) are possible child pornography. I recognized file (g) as a video clip of a female under the age of eighteen performing oral sex on and masturbating a male. I have encountered this child pornography video clip in prior child exploitation investigations.

14. During the downloads, "Alex1007" initiated a private message session with SS/A Buduris' undercover persona. WinMX supports private messages, which are messages that only the sender and receiver can see. During the private message session, "Alex1007" identified himself as a twenty-four year old male from Florida. SS/A Buduris identified herself as a twenty-five year old female from Illinois. "Alex1007" indicated his favorite age range was ten-thirteen years old. SS/A Buduris typed "I like ur alex pics", referring to downloaded files (b) and (c). "Alex1007" replied "Thank you sweety, download anything you like honey."

15. SS/A Buduris identified the IP address in use by "Alex1007" as 4.235.171.245. An IP address is a unique number assigned to a computer or device connected to the Internet. Because no two computers or devices connected to the Internet can

---

[1] The download of this file was not completed due to SS/A Buduris losing connectivity with "Alex1007". 6.65 megabytes of 8.5 megabytes was downloaded resulting in a 33 second video clip.

have the same IP address at the same time, a specific user can be identified. SS/A Buduris identified the IP address as being assigned to Level 3 Communications.

16. A summons was issued to Level 3 Communications to identify the user of the IP address at the time the files were being downloaded. The response to the summons indicated that at the time of the offense, the IP address was in use by user name "cookie67@auntwillie.com", an Earthlink subscriber. The response indicated the IP address was assigned to a telephone modem and identified the calling number as 863-382-6971.

17. A summons was issued to Earthlink to identify the subscriber. The response to the summons identified the subscriber, "cookie67@auntwillie.com", as:

Alicia Peters
P.O. Box 1595
Sebring, FL
Home Phone Number: 863-382-6971

18. I conducted a search for Alicia Peters, Sebring, FL in the Yellowpages.com online directory. I identified a listing for her at 7611 U.S. Highway 27 South, Sebring, Florida, telephone number 863-382-6971.

19. I conducted a check of the Florida Department of Highway Safety and Motor Vehicles Driver and Vehicle Information Database. I identified a driver license issued to Alicia Peters at the above post office box address. The database also showed a driver license

issued to Paul Peters III (58 years old) and Paul Peters IV (19 years old), both at 7611 U.S. Highway 27 South, Sebring, Florida.

20. SS/A Buduris took a screen shot of the files "Alex1007" was offering for download. WinMX displays not only the file name being offered, but also the full file path on the hard drive. The path to the image files being offered for download was: C:\WINDOWS\Profiles\erevain\Desktop\Paul's Stuff\Paul's DLs\stuff\

21. According to the Highlands County Property Appraiser website, 7611 U.S. Highway 27 South, Sebring, Florida is owned by Crutchfield Groves, Inc. The property appraiser record shows two buildings on the parcel. The larger of the two buildings is listed as having an unfinished interior, concrete floor, and a half bath. The smaller of the two is listed as having interior drywall, two bedrooms, a full bathroom, and central air.

22. On March 1, 2006, ICE S/A Van Lindsey conducted aerial surveillance of 7611 U.S. Highway 27 South, Sebring, Florida, and observed that the two buildings are physically attached and are under the same roof. S/A Lindsey stated that the buildings are indistinguishable as separate and appear to be one structure.

23. A wage and hour check revealed Henry Crutchfield, Inc., employed Paul Peters III at least from the first quarter of 2004 through the latest reporting time frame available, the fourth quarter of 2005.

24. Based on the foregoing facts, I believe there is evidence of violations of 18 U.S.C. § 2252 (Certain activities relating to material involving the sexual exploitation of minors) present and shall be found on the computers used or accessed at 7611 U.S. Highway 27 South, Sebring, Florida. Specifically, I believe that 7611 U.S. Highway 27 South, Sebring, Florida, is the site of knowing transmission and possession of matters containing visual depictions that have been shipped or transported in interstate and/or foreign commerce by any means, including by computer, and the production of which involves the use of a minor engaging in sexually explicit conduct and such visual depiction is of such conduct.

Further your affiant sayth naught.

Brian P. Ray
Special Agent
U.S. Immigration and
Customs Enforcement

Subscribed and sworn to before me this _____ day of March 2006, at Fort Pierce, Florida.

Frank J. Lynch, Jr.
United States Magistrate Judge